How Firewall Protection Works

Firewall protection works by blocking certain types of traffic between a source and a destination.

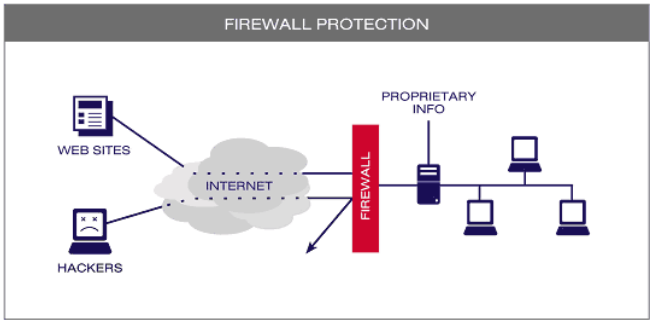
All network traffic has a source, a destination, and a protocol. This protocol is usually TCP, UDP, or ICMP.

If this protocol is TCP or UDP, there is a source port and a destination port. Most often the source port is a random port and the destination port is a well-known port number. For example, the destination port for HTTP is 80 and the destination port for DNS is 53.

If the protocol is ICMP, there is also an ICMP message type. The most common ICMP message types are Echo Request and Echo Reply.

Firewall protection works by allowing the network security administrator to choose which protocols and ports or message types to allow — and which ones to deny.

Firewall Protection: Denying Inbound



Most firewall configurations should deny **all** inbound traffic to **all** *internal* IP addresses.

Servers which must accept incoming connections should be placed on a DMZ network.

Modern firewalls will allow packets to come into the network which are responses to outbound traffic. What this means is that if you connect to a web server across the Internet, the firewall will automatically allow the responses from the web server to return to you.

Inbound restrictions are the main security value provided by firewalls.

Firewall Protection: Denying Outbound

Some network security administrators deny outbound traffic.

This is most often done to restrict users to approved protocols and prevent them from using unapproved protocols. This usually means preventing users from using online chat systems or preventing them from sending outbound e-mail.

Outbound restrictions are often vulnerable to work-arounds. These work-arounds require time and effort on the part of the network user, which limits the number of users who can utilize unapproved protocols. Outbound restrictions seldom, if ever, work entirely as designed.

Example Firewall Protection: Denying Inbound `ping`

The `ping` command sends out ICMP Echo Request messages and expects ICMP Echo Reply messages in response.

If you configure a firewall between the source and the destination to block ICMP Echo Request messages from the source to the destination, the `ping` command will fail.

Similarly, if you configure a firewall between the source and the destination to block ICMP Echo *Reply* messages from the *destination* to the *source*, the `ping` command will also fail.

The `ping` command can allow a potential attacker to map your network. Disabling inbound Echo Request messages prevents the use of the `ping` command to map your network.

Example Firewall Protection: Blocking Outbound E-mail

Internet e-mail uses the SMTP protocol. SMTP servers answer on TCP port 25.

If you block outbound TCP port 25 from your network, users will not be able to send outbound e-mail — except through your approved e-mail servers.

However, a *sophisticated user* who operates their own mail server could configure their mail server to respond on another port, in addition to port 25. This would be an effective work-around your security policy.